



DEPARTMENT OF JUSTICE

28 CFR Part 16

[CPCLO Order No. 008-2021]

Privacy Act of 1974; Implementation

AGENCY: United States Department of Justice, Justice Management Division (JMD).

ACTION: Notice of proposed rulemaking.

SUMMARY: The Department of Justice (Department or DOJ), Justice Management Division (JMD), in the Notices section of this issue of the *Federal Register*, is publishing a new system of records, “Security Monitoring and Analytics Service Records,” JUSTICE/JMD-026. In this notice of proposed rulemaking, DOJ proposes to exempt this system of records from certain provisions of the Privacy Act to avoid interference with efforts to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of information, information systems, and networks of DOJ and external federal agency subscribers. For the reasons provided below, the Department proposes to amend its Privacy Act regulations by establishing an exemption from certain provisions of the Privacy Act for this system of records. Public comment is invited.

DATES: Comments must be received by [INSERT DATE 30 AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may send comments by any of the following methods:

- Federal eRulemaking Portal: <http://www.regulations.gov>. When submitting comments electronically, you must include the CPCLO Order No. in the subject box. Please note that the Department is requesting that electronic comments be submitted before midnight Eastern Standard Time on the day the comment period closes because <http://www.regulations.gov> terminates the public’s ability to submit comments at that time. Commenters in time zones other than Eastern

Standard Time may want to consider this so that their electronic comments are received.

- Mail: United States Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, Office of Privacy and Civil Liberties, 145 N St. NE, Suite 8W.300, Washington, DC 20530. All comments sent via regular or express mail will be considered timely if postmarked on the day the comment period closes. To ensure proper handling, please reference the CPCLO Order No. in your correspondence.

Posting of Public Comments: Interested persons are invited to participate in this rulemaking by submitting written data, views, or arguments on all aspects of this rule by one of the methods and by the deadline stated above. All comments must be submitted in English, or accompanied by an English translation. The Department also invites comments that relate to the economic, environmental, or federalism effects that might result from this rule. Comments that will provide the most assistance to the Department in developing these procedures will reference a specific portion of the rule, explain the reason for any recommended change, and include data, information, or authority that support such recommended change.

Please note that all comments received are considered part of the public record and made available for public inspection at www.regulations.gov. Such information includes personally identifying information (PII) (such as your name, address, etc.). Interested persons are not required to submit their PII in order to comment on this rule. However, any PII that is submitted is subject to being posted to the publicly-accessible www.regulations.gov site without redaction.

Confidential business information clearly identified in the first paragraph of the comment as such will not be placed in the public docket file.

The Department may withhold from public viewing information provided in comments that they determine may impact the privacy of an individual or is offensive. For additional information, please read the Privacy Act notice that is available via the link in the footer of <http://www.regulations.gov>. To inspect the agency's public docket file in person, you must make an appointment with the agency. Please see the "FOR FURTHER INFORMATION CONTACT" paragraph, below, for agency contact information.

FOR FURTHER INFORMATION CONTACT: Nickolous Ward, DOJ Chief Information Security Officer, (202) 514-3101, 145 N Street NE, Washington, DC 20530.

SUPPLEMENTARY INFORMATION:

In accordance with the Federal Information Security Modernization Act of 2014, among other authorities, agencies are responsible for complying with information security policies and procedures requiring information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems. *See, e.g.*, 44 U.S.C. 3554 (2018). Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017), directs agency heads to show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services. Office of Management and Budget (OMB) Memorandum M-19-16, Centralized Mission Support Capabilities for the Federal Government (April 26, 2019), establishes the framework for implementing the "Sharing Quality Services" across agencies. The Economy Act of 1932, as amended, 31 U.S.C. 1535, authorizes agencies to enter into agreements to obtain supplies or services from another agency. Consistent with these authorities, the JMD, Office of the Chief Information Officer (OCIO), Cybersecurity Services Staff (CSS), developed the Security Monitoring and Analytics Service (SMAS) system to provide

DOJ-managed information technology service offerings to other federal agencies wishing to leverage DOJ's cybersecurity services, referred to as "external federal agency subscribers." This system provides external federal agency subscribers with the technical capability to protect their data from malicious or accidental threats using a DOJ-managed system. Elsewhere in the Federal Register, JMD published a notice of a new system of records titled, "Security Monitoring and Analytics Service Records," JUSTICE/JMD-026, to provide the public notice of the records maintained by DOJ while implementing SMAS.

In this rulemaking, the Department proposes to exempt JUSTICE/JMD-026 from certain provisions of the Privacy Act in order to avoid interference with the responsibilities of the Department to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of external federal agency subscribers' information and information systems. Additionally, the Department proposes to exempt JUSTICE/JMD-026 from certain provisions to assist DOJ and external federal agency subscribers with protecting such data and ensuring the secure operation of information systems.

Executive Orders 12866 and 13563—Regulatory Review

In accordance with 5 U.S.C. 552a(j) and 552a(k), this proposed action is subject to formal rulemaking procedures by giving interested persons an opportunity to participate in the rulemaking process "through submission of written data, views, or arguments," pursuant to 5 U.S.C. 553. This proposed rule will promulgate certain Privacy Act exemptions for a DOJ system of records titled, "Security Monitoring and Analytics Service Records," JUSTICE/ JMD-026. This proposed rule does not raise novel legal or policy issues, nor does it adversely affect the economy, the budgetary impact of entitlements, grants, user fees, loan programs, or the rights and obligations of recipients thereof in a material way. The Department of Justice has determined that this rule is not a

“significant regulatory action” under Executive Order 12866, section 3(f), and accordingly this rule has not been reviewed by the Office of Information and Regulatory Affairs within the Office of Management and Budget pursuant to Executive Order 12866.

Regulatory Flexibility Act

This proposed rule will only impact Privacy Act-protected records, which are personal and generally do not apply to an individual’s entrepreneurial capacity, subject to limited exceptions. Accordingly, the Chief Privacy and Civil Liberties Officer, in accordance with the Regulatory Flexibility Act (5 U.S.C. 605(b)), has reviewed this regulation and by approving it certifies that this regulation will not have a significant economic impact on a substantial number of small entities.

Small Business Regulatory Enforcement Fairness Act of 1996 (Subtitle E–Congressional Review Act)

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996, 5 U.S.C. 801 *et seq.*, requires the Department to comply with small entity requests for information and advice about compliance with statutes and regulations within the Department’s jurisdiction. Any small entity that has a question regarding this document may contact the person listed in “FOR FURTHER INFORMATION CONTACT” paragraph, above. Persons can obtain further information regarding SBREFA on the Small Business Administration’s Web page at <https://www.sba.gov/advocacy>. This proposed rule is not a major rule as defined by 5 U.S.C. 804 of the Congressional Review Act.

Executive Order 13132–Federalism

This proposed rule will not have substantial direct effects on the States, on the relationship between the national government and the States, or on distribution of power and responsibilities among the various levels of government. Therefore, in accordance

with Executive Order 13132, it is determined that this rule does not have sufficient federalism implications to warrant the preparation of a Federalism Assessment.

Executive Order 12988–Civil Justice Reform

This proposed regulation meets the applicable standards set forth in sections 3(a) and 3(b)(2) of Executive Order 12988 to eliminate drafting errors and ambiguity, minimize litigation, provide a clear legal standard for affected conduct, and promote simplification and burden reduction.

Executive Order 13175–Consultation and Coordination With Indian Tribal Governments

This proposed rule will have no implications for Indian Tribal governments. More specifically, it does not have substantial direct effects on one or more Indian tribes, on the relationship between the Federal government and Indian tribes, or on the distribution of power and responsibilities between the Federal government and Indian tribes. Therefore, the consultation requirements of Executive Order 13175 do not apply.

Unfunded Mandates Reform Act of 1995

This proposed rule will not result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of \$100,000,000, as adjusted for inflation, or more in any one year, and it will not significantly or uniquely affect small governments. Therefore, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Paperwork Reduction Act

The Paperwork Reduction Act of 1995, 44 U.S.C. 3507(d), requires the Department to consider the impact of paperwork and other information collection burdens imposed on the public. There are no current or new information collection requirements associated with this proposed rule.

List of Subjects in 28 CFR Part 16

Administrative Practices and Procedures, Courts, Freedom of Information, and the Privacy Act.

Pursuant to the authority vested in the Attorney General by 5 U.S.C. 552a and delegated to me by Attorney General Order 2940-2008, the Department of Justice proposes to amend 28 CFR part 16 as follows:

Part 16-PRODUCTION OR DISCLOSURE OF MATERIAL OR INFORMATION

1. The authority citation for part 16 continues to read as follows:

Authority: 5 U.S.C. 301, 552, 552a, 553; 28 U.S.C. 509, 510, 534; 31 U.S.C. 3717.

Subpart E – Exemption of Records Systems Under the Privacy Act

2. Amend § 16.76 by adding paragraphs (e) and (f) to read as follows:

§16.76 Exemption of Justice Management Division.

* * * * *

(e) The following system of records is exempted from 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (H), and (I); and (f): Department of Justice Security Monitoring and Analytics System (JUSTICE/ JMD-025). These exemptions apply only to the extent that information in this system is subject to exemption pursuant to 5 U.S.C. 552a(k)(2).

Where DOJ determines compliance would not appear to interfere with or adversely affect the purpose of this system to ensure that the Department can track information system access and implement information security protections commensurate with the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of DOJ information and information systems, the applicable exemption may be waived by the DOJ in its sole discretion.

(f) Exemptions from the particular subsections are justified for the following reasons:

(1) From subsection (c)(3), the requirement that an accounting be made available to the named subject of a record, because this system is exempt from the access provisions of subsection (d). Also, because making available to a record subject the accounting of disclosures of records concerning the subject would specifically reveal investigative interests in the records by the DOJ, external federal agency subscribers, or other entities that are recipients of the disclosures. Revealing this information could compromise sensitive information or interfere with the overall law enforcement process by revealing a pending sensitive cybersecurity investigation. Revealing this information could also permit the record subject to obtain valuable insight concerning the information obtained during any investigation and to take measures to impede the investigation, e.g., destroy evidence or alter techniques to evade discovery.

(2) From subsection (d)(1), (2), (3) and (4), (e)(4)(G) and (H), and (f) because these provisions concern individual access to and amendment of certain law enforcement and sensitive records, compliance of which could alert the subject of an authorized law enforcement activity about that particular activity and the interest of the DOJ, external federal agency subscribers, and/or other entities that are recipients of the disclosure. Providing access could compromise sensitive information, or reveal sensitive cybersecurity investigative techniques; provide information that would allow a subject to avoid detection; or constitute a potential danger to the health or safety of law enforcement personnel or confidential sources.

(3) From subsection (e)(1) because it is not always possible to know in advance what information is relevant and necessary for law enforcement purposes. The relevance and utility of certain information that may have a nexus to cybersecurity threats may not always be fully evident until and unless it is vetted and matched with other information necessarily and lawfully maintained by the DOJ, external federal agency subscribers, or other entities.

(4) From subsection (e)(4)(I), to the extent that this subsection is interpreted to require more detail regarding the record sources in this system than has been published in the *Federal Register*. Should the subsection be so interpreted, exemption from this provision is necessary to protect the sources of law enforcement information.

Dated: July 20, 2021

Peter A. Winn
Acting Chief Privacy and Civil Liberties Officer
United States Department of Justice

[FR Doc. 2021-15884 Filed: 7/29/2021 8:45 am; Publication Date: 7/30/2021]